BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi terus berkembang seiring dengan perubahan zaman, perkembangan teknologi ini dapat mempengaruhi berbagai kegiatan dalam bidang kehidupan manusia. Salah satunya pertukaran informasi dan komunikasi data yang sering dilakukan. Jika dalam pertukaran informasi keamanannya tidak terjaga, maka pihak lain dapat memanfaatkan informasi yang akan merugikan pihak yang berhak atas informasi tersebut (Prasetio. dkk., 2018). Namun kebocoran data tidak hanya terjadi dari kesalahan atau kelemahan sistem melainkan terdapat juga kesalahan dari manusia (Seputra. dkk., 2020).

Keamanan informasi sangat dibutuhkan, untuk mengamankan suatu informasi dapat dilakukan dengan teknik menyembunyikan pesan menjadi sesuatu yang tidak terbaca yakni kriptografi. Kriptografi adalah bidang ilmu yang mempelajari tentang penyembunyian informasi berupa data yang sulit terbaca oleh orang yang tidak memiliki kunci dekripsi.

Tidak hanya digunakan untuk keamanan, kriptografi dapat digunakan dalam tindak kejahatan, salah satunya yakni malware yang dapat mengenkripsi suatu data di dalam komputer atau sistem komputer yang disebut dengan Ransomware.

Ransomware menyebar melalui e-mail Phising, tautan berbahaya, download dari web yang mencurigakan, dan perangkat yang saling terhubung. Ransomware terdapat pada penyedia film, game, anime, dan segala hal yang berbayar tetapi gratis untuk didapatkan dalam web penyedia. hal ini akan terjadi, ketika salah dalam menekan tombol atau link unduh *file* sehingga menginstal sebuah aplikasi

yang tidak dikenal, yang mengakibatkan format beberapa *file* data pengguna berubah, dengan demikian *file* data tidak dapat dibuka karena mengalami *corrupt*.

Untuk mengembalikan *file corrupt*, dibutuhkan kunci untuk mendekripsi *file* tersebut, untuk mendapatkan kunci, tidaklah mudah, pihak pembuat ransomware menyediakan *file* (.txt) yang berisi pesan yakni meminta imbalan berupa uang, akan tetapi dengan membayar tidak menjadi jaminan *file* akan kembali seperti semula (Ganesan. dkk., 2019).

Secara umum, kriptografi dibagi menjadi dua jenis: kriptografi simetris dan kriptografi asimetris. Kriptografi Hill cipher adalah salah satu contoh kriptografi simetris. Bentuk kunci dari kriptografi ini adalah berbentuk matriks. Hill cipher adalah kriptografi klasik yang berdasar pada transformasi matriks yang rentan terhadap serangan known-*plaintext* (Toorani, 2009).

Dalam meningkatkan keamanan Hill cipher, dapat dikembangkan dengan mengkombinasikan antara kriptografi Hill cipher dengan kriptografi yang memiliki kunci asimetris. mengkombinasikan dua kriptografi bertujuan untuk memperkuat suatu keamanan informasi, yang nantinya dapat menghasilkan keteracakan *ciphertext* yang baik, salah satu contoh kriptografi asimetris adalah kriptografi ElGamal.

Kriptografi ElGamal memiliki tingkat keamanan yang tinggi, karena dalam proses enkripsi ElGamal, blok yang sama dienkripsi dua kali menggunakan proses yang berbeda, yang menghasilkan *ciphertext* (Caroline, 2011).

Penelitian mengenai Kriptografi Hill cipher dan algoritma ElGamal pernah dilakukan oleh Lisda Juana Pangaribuan pada tahun 2018 yang berjudul “Kriptografi Hybrid Algoritma Hill Cipher Dan Rivest Shamir Adleman (RSA)

Sebagai Pengembangan Kriptografi Kunci Simetri". Pada penelitian ini, Lisda Juana Pangaribuan melakukan enkripsi menggunakan kriptografi *hybrid* yang digunakan untuk mengembangkan keamanan kunci simetris (Pangaribuan, 2018).

Penelitian yang dilakukan oleh Bella Ariska, Suroso, Jon Endri pada tahun 2018 yang berjudul "Rancangan Kriptografi Hybrid Kombinasi Metode Vigenere Cipher Dan Elgamal Pada Pengamanan Pesan Rahasia". Pada penelitian ini, Bella Ariska, Suroso, Jon Endri melakukan rancangan kriptografi hybrid yang digunakan untuk pengamanan pesan rahasia (Ariska. dkk., 2018).

Penelitian lain tentang kriptografi dilakukan oleh Dian Rachmawati, Amer sharif, dan ericko, tahun 2019 yang berjudul Hybrid Cryptosystem Combination Algorithm Of Hill Cipher 3x3 and Elgamal To Secure Instant Messaging For Android. Pada penelitian ini dilakukan teknik pengriman pesan menggunakan ElGamal dalam mengamankan kunci simetris dan hill cipher yang digunakan untuk mengenkripsi pesan atau *plaintext* yang dikirimkan.

Berdasarkan ketiga penelitian tersebut, penulis tertarik untuk mengkombinasikan kedua kriptografi yakni Hill cipher dan ElGamal. Sehingga penulis ingin mengkaji penelitian dengan judul "Kriptografi Hybrid Metode Hill Cipher dan Elgamal dalam Meningkatkan Keamanan Pesan. Kriptografi yang digunakan yakni kriptografi simetris menggunakan Hill Chiper yang dikombinasikan dengan kriptografi asimetris menggunakan Kriptografi Elgamal.

1.2.Rumusan Masalah

Berdasarkan latar belakang di atas, dapat dirumuskan masalah sebagai berikut:

a. Bagaimana prosedur dalam menyandikan pesan dengan menggunakan kriptografi *hybrid* Metode Hill cipher dan ElGamal ?
b. Bagaimana performa metode *hybrid* dibandingkan dengan menggunakan salah satu metode kriptografi ?

1.3. Batasan Masalah

Dalam pengerjaan tugas akhir ini, adapun batasan masalah yang diperhatikan antara lain :

a. Penelitian dilakukan hanya menggunakan dua metode kriptografi yakni metode Hill cipher dan Elgamal.
b. *Data* yang digunakan dalam penelitian ini yakni menggunakan pesan atau berbentuk *text*.
c. Bahasa pemrograman yang digunakan adalah bahasa pemrograman java.

1.4. Tujuan Penelitian

Adapun tujuan penelitian sebagai berikut :

a. Mengetahui proses enkripsi dan dekripsi dengan menggunakan metode *hybrid* yang dapat menyembunyikan pesan dari pihak ketiga.
b. Mengetahui perbandingan performa enkripsi dan dekripsi dengan antara satu metode dengan metode *hybrid* (dua metode).

1.5. Manfaat Penelitian

Berdasarkan dari tujuan penelitian, maka menghasilkan manfaat penelitian, adapun manfaat penelitian ini adalah sebagai berikut :

1.5.1. Manfaat Teoritis

Manfaat teoritis yang diperoleh dari penelitian ini, sebagai berikut :

a. Sebagai acuan bagi mahasiswa dalam mengembangkan ilmu pengetahuan yang berkaitan dengan keamanan data *text* menggunakan metode kriptografi, baik kriptografi simetris maupun kriptografi asimetris ataupun kombinasi dua metode kriptografi.
b. Sebagai acuan untuk peneliti lainnya yang ingin mengembangkan penelitian terkait keamanan data dengan menggunakan kriptografi *hybrid* metode Hill cipher dan ElGamal dalam meningkatkan keamanan pesan rahasia.
c. Menjadikan penelitian ini, sebagai sumber informasi tambahan bagi peneliti yang ingin melakukan penelitian sejenis atau bahkan menjadikan dasar untuk penelitian-penelitian yang terkait dengan kriptografi.

1.5.2. Manfaat Praktis

Selain manfaat teoritis, terdapat beberapa manfaat praktis sebagai berikut :

a. Hasil penelitian ini dapat di implementasikan oleh pembaca dalam menambah wawasan terkait keamanan data *text*, sehingga lebih waspada dalam berselancar di internet.
b. Hasil penelitian ini dapat di terapkan oleh peneliti dalam melakukan implementasi kriptografi *hybrid* metode Hill cipher dan ElGamal dalam meningkatkan keamanan pesan rahasia.